UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/875,446	06/05/2001	Davin J. Fifield	43576.830012.US1	5057

7590 09/06/2007

Brian Kinnear
Holland & Hart LLP
555 Seventeenth Street
Suite 3200
Denver, CO 80202

EXAMINER	
TRAN, QUOC A	

ART UNIT	PAPER NUMBER
2176	

MAIL DATE	DELIVERY MODE
09/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

mn

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/875,446
Filing Date: June 05, 2001
Appellant(s): FIFIELD ET AL.

James A. Sheridan
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 02-12-2007 appealing from the Office action mailed 06-14-2006.

1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

US006091835A	Smithies et al.	filed 02-17-1998
US006901509B1	Kocher	filed 02-22-2000
US006336188B2	Blake-Wilson et al.	filed 05-01-1998

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

DETAILED ACTION

This is a Final rejection in response to arguments filed on March 22, 2006. Claims 1-20 are pending and rejected in this action. Effective date is 5/5/2000.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1, 3-6, 7- 9, 11-15, 17 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smithies et al (US 6091835, filed Feb 1998), in view of Kocher (US 6901509, filed Feb 2000).

Regarding claim 1, 7, 8, 9, 17 and 19, Smithies teaches *performing a first hash operation on the electronic transcript to generate a representation of the contents of the electronic transcript.* Smithies discloses a method for transcribing electronic affirmations (Title), where the hash encoding is equal to "document checksum" (col 14, lines 14-17), and a checksum is created of the document transcript object (col 8, lines 25-38).

Smithies teaches concatenating data to the representation of the contents of the electronic transcript, said data identifying a user; digitally signing the notary record. *Smithies discloses a digital signature that is added to the principal transcript object after verification by the transcript generator (col 9, lines 40-44).*

Smithies teaches *providing for the recording and time stamping by a digital notary service of the representation of the contents of the electronic transcript and the data; obtaining a notary record from he digital notary service of the time stamping.* Smithies discloses including the affirming party's input in verifying the time stamp data as evidence that the affirming party validly affirmed the document (col 13, line 30 – col 14, line 4).

Smithies teaches *forming an electronically signed electronic transcript by bundling the digitally signed notary record with the electronic transcript and with the data identifying the user.* For example, Smithies discloses a system that adds the signature information to the principal transcript to (col 9, lines 40-45) and creates a resulting transcript with a private key that verifies the identity of a party, including an affirmation (col 8, lines 1-15).

Smithies does not expressly teach, but Kocher teaches *performing a second hash operation on the data concatenated to the representation, the second hash operation generating a representation of the contents of the electronic transcript and the data.* Kocher discloses a method for demonstrating and confirming the status of a digital certificate and other data (Title), where hashing the result of the previous hash suggests that a second hash is performed on the results of the first has operation (col 10, lines 15-25).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Smithies to include hashing the result of the previous hash suggests that a second hash

is performed on the results of the first has operation as taught by Kocher, providing the benefit of demonstrating and confirming the status of a digital certificates and other data on a computer-implemented method (Kocher, Abstract section) and calling the transcript generator module to affirm a previously saved transcript object (Smithies, col 12, lines 40-42).

Regarding claim 3, 11, Smithies teaches data includes a user name uniquely identifying the user (ie., affirming party, identifying party entering affirming data, password)(col 7, lines 23-30).

Regarding claim 4, 12, Smithies teaches data includes a user number associated with the user (ie., ... unique secret number ...)(col 7, lines 45-50).

Regarding claim 5, 13, Smithies teaches data includes a recipient's name (ie., ... party's name)(col 7, lines 50-52).

Regarding claim 6, 14, Smithies teaches data includes a unique identifier, which uniquely identifies the transcript. Smithies teaches encoding a document or transaction with information that verifies the integrity of the document (col 14, lines 5-21) and identification data by system that transcript generator collects (col 13, lines 52-60).

Regarding claim 15, Smithies teaches " file contains ... transcript" (ie., transcript object can be encrypted in a statement file)(col 8, lines 25-30).

Claims 2, 10, 16, 18 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smithies et al (as cited above), in view of Kocher (as cited above), further in view of Blake-Wilson et al (US 6336188, filed May 1998).

Regarding claim 2, 10, Smithies in view of Kocher does not teach, but Blake-Wilson teaches "has operation is a RIPEMD-160 hash operation" (ie., hash function, RIPEMD-160)(col 5, lines 25-40).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Smithies in view of Kocher to include RIPEMD hashing as taught by Blake-Wilson, providing the benefit of authentication key agreement protocols used in digital data communication systems (Blake-Wilson, col 1, lines 4-5, lines 60-65).

Regarding claims 16, 18, 20, Smithies teaches "file excludes page numbers, line numbers, headers, and footers" (ie., the transcript file does not indicate the presence of page numbers, line numbers, headers or footers)(Summary section). Additionally, has been very common to one or ordinary skill in the art at the time of the invention to use word processor software applications (ie., Microsoft Word,... etc) that allow for toggling page number, line numbers, headers and footers off and on depending on the user's choice.

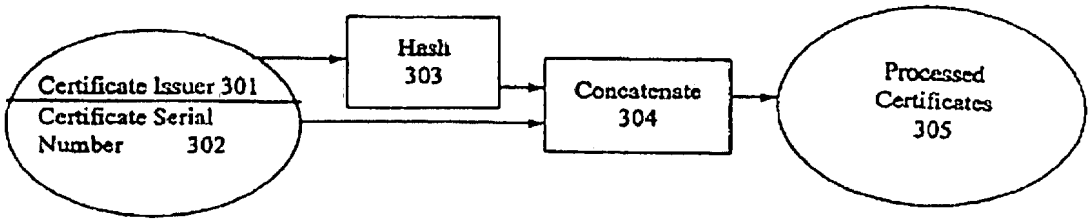
(10) Response to Argument

Brief description of cited prior arts:

Smithies (hereinafter Smithies'835), discloses a method and system for gathering and recording information concerning the affirmation of an electronic document. Such as system should operate with a capacity to generate a comprehensive transcript or record of the facts and circumstances associated with a party's action as they "sign" and "affirm" an electronic document (see Smithies'835 col. 6 lines 55-65). The term "affirm" as used herein includes the act of signing a document, electronic or otherwise by any biometric, infometric or cryptographic means. The party may enter a handle, pointer or other access to a private key, which can be used to encrypt representations of the document and resulting transcript; this key will serve to verify the identity of the party. Also the term "affirmation" may also extend to events, (such as the transmission of a file or document), the occurrence of which may be recorded and stored in lieu of a traditional signature (see Smithies'835 col. 7 line 60 through col. 9, line 15). In addition, Smithies'835 method and system applies Authentication Policy Component (APC) digitally signed by its creator authorizer through the use of private asymmetric key; includes the APC check through document checksum. The process of generating a checksum is a known mathematical process, which takes the sequence of characters in a document and calculates a number, which is mathematically related to the sequence. If the sequence of characters in a document is altered or changed, the checksum created with the revised document will not match the checksum created with the original version. By comparing a later calculated checksum to the original, the system of the present invention can monitor and determine whether a change has

occurred in a document. For purposes of an exemplary embodiment, the present invention can use any checksumming software, such as those employing the RSA, Inc. MD5 algorithm or the Secure Hash Algorithm SHA-1 (see Smithies'835 col. 23 line 65 through col. 24 line 15).

Kocher (hereinafter Kocher'509) discloses methods and apparatuses for constructing efficient cryptographically secure assertions as to whether candidate items are present on a list, includes the construction of a hash tree, wherein a verifier can determine the validity of the digital signature on the root node, and provides cryptographic assurance that the candidate data item is not on the list (see Kocher'509 col. 5 line 65 through col. 6 line 15). In addition, Kocher'509 in fig. 3 and col. 6 lines 40-50, discloses a particular preprocessing technique appropriate for data items such as digital certificates. The certificate issuer name 301 is hashed at step 303, and at step 304, the hashed issuer name is concatenated with the certificate serial number 302 to produce the processed digital certificate 305. (The serial number could also be hashed before concatenation.) For example, a certificate with a 32-bit (4-byte) serial number 123456789 whose CA name is "Sample CA" would have a 24-byte list entry consisting of SHA ("Sample CA") followed by the byte representation of 123456789. In particular, the hexadecimal representation would be: E2 CA 64 56 40 BE 99 AC CA 9D 3A 9B 02 97 0D 1E F2 95 8E A0 07 5B CD 15.)



Blake-Wilson (hereinafter Blake-Wilson'188) discloses an Authenticated Key (AK) protocol utilizing a hash function such as SHA-1 (see Blake-Wilson'188 col. 5 lines 20-35).

Beginning on page 13 of the appeal brief (hereinafter the brief), Appellant argues the following issues, which are accordingly addressed below.

First: Appellant argues, **Smithies'835 teaches only a single hash operation on a document, and has no teaching or suggestion of a second hash operation on data concatenated to a presentation as required by claim 1** (see the brief page 14 para 2- the same arguments are substantially repeated for claims 2-20 pending –see the brief pages 17-22).

The examiner respectfully disagrees.

As discuss in the rejection above, Specifically, **Smithies'835** discloses a method and system for gathering and recording information concerning the affirmation of an electronic document. Such as system should operate with a capacity to generate a comprehensive transcript or record of the facts and circumstances associated with a party's action as they "sign" and "affirm" an electronic document (see Smithies'835 col. 6 lines 55-65). The term "affirm" as used herein includes the act of signing a document, electronic or otherwise by any biometric, infometric or cryptographic means. The party may enter a handle, pointer or other access to a private key, which can be used to encrypt representations of the document and resulting transcript; this key will serve to verify the identity of the party. Also the term "affirmation" may also extend to events, (such as the transmission of a file or document), the occurrence of which

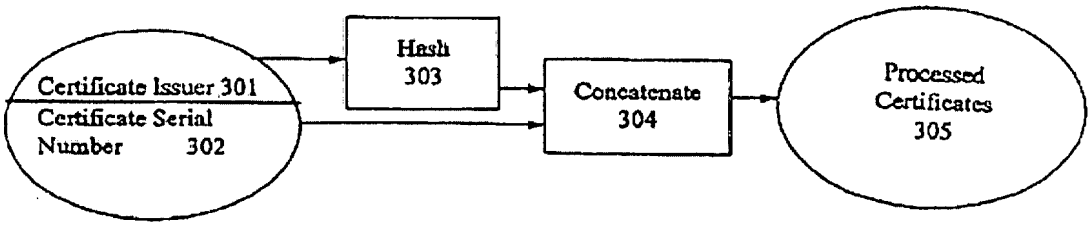
may be recorded and stored in lieu of a traditional signature (see Smithies'835 col. 7 line 60 through col. 9, line 15). In addition, Smithies'835 method and system applies Authentication Policy Component (APC) digitally signed by its creator authorizer through the use of private asymmetric key; includes the APC check through document checksum. The process of generating a checksum is a known mathematical process, which takes the sequence of characters in a document and calculates a number, which is mathematically related to the sequence. If the sequence of characters in a document is altered or changed, the checksum created with the revised document will not match the checksum created with the original version. By comparing a later calculated checksum to the original, the system of the present invention can monitor and determine whether a change has occurred in a document. For purposes of an exemplary embodiment, the present invention can use any checksumming software, such as those employing the RSA, Inc. MD5 algorithm or the Secure Hash Algorithm SHA-1 (see Smithies'835 col. 23 line 65 through col. 24 line 15).

Using the broadest reasonable interpretation, the examiner equates the claimed **first hash** as equivalent to uses of the Secure Hash Algorithm SHA-1, since SHA-1 is used for both "sign" and "affirm"; SHA-1 is hashed when "sign", and "affirm" an electronic document (see Smithies'835 col. 6 lines 55-65). The term "affirm" as used herein includes the act of signing a document, electronic or otherwise by any biometric, infometric or cryptographic means. The party may enter a handle, pointer or other access to a private key, which can be used to encrypt representations of the document and resulting transcript; this key will serve to verify the identity of the party; and SHA-1 is hashed when applies Authentication Policy Component (APC) digitally signed by its creator authorizer through the use of private asymmetric key; includes the

APC check through document checksum. The process of generating a checksum is a known mathematical process, which takes the sequence of characters in a document and calculates a number, which is mathematically related to the sequence. If the sequence of characters in a document is altered or changed, the checksum created with the revised document will not match the checksum created with the original version as taught by Smithies'835 (see Smithies'835 col. 6 lines 55-65, col. 7 line 60 through col. 9, and line 15col. 23 line 65 through col. 24 line 15).

In addition, Smithies'835 does not explicitly teach **a second hash operation on data concatenated to a presentation.** Using the broadest reasonable interpretation, it is noted Smithies'835 teaches the Secure Hash Algorithm SHA-1, but does not expressly distinguish first and second hash; since SHA-1 is used for both "sign" and "affirm"; SHA-1 is hashed when "sign", and "affirm" an electronic document. It would have been obvious to one of ordinary skill in the art at the time of the invention to equates the **first hash and second hash** as equivalent to SHA-1 is used for both "sign" and "affirm". However, for further support, Kocher'509 discloses methods and apparatuses for constructing efficient cryptographically secure assertions as to whether candidate items are present on a list, includes the construction of a hash tree, wherein a verifier can determine the validity of the digital signature on the root node, and provides cryptographic assurance that the candidate data item is not on the list (see Kocher'509 col. 5 line 65 through col. 6 line 15). In addition, Kocher'509 in fig. 3 and col. 6 lines 40-50, discloses a particular preprocessing technique appropriate for data items such as digital certificates. The certificate issuer name 301 is hashed at step 303, and at step 304, the hashed issuer name is concatenated with the certificate serial number 302 to produce the processed digital certificate 305. (The serial number could also be hashed before concatenation.) For example, a certificate

with a 32-bit (4-byte) serial number 123456789 whose CA name is "Sample CA" would have a 24-byte list entry consisting of SHA ("Sample CA") followed by the byte representation of 123456789. In particular, the hexadecimal representation would be: E2 CA 64 56 40 BE 99 AC CA 9D 3A 9B 02 97 0D 1E F2 95 8E A0 07 5B CD 15.)



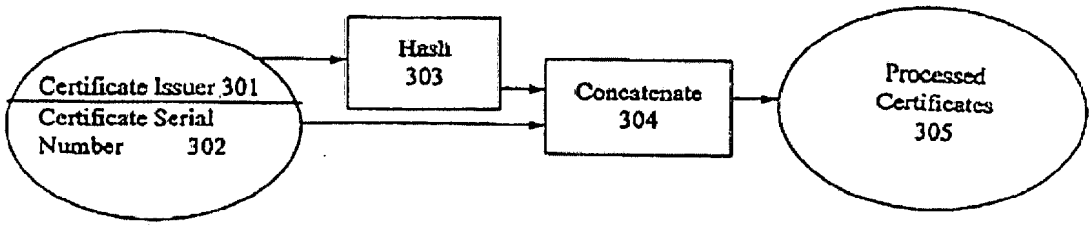
Using the broadest reasonable interpretation, the examiner equates the claimed **a second hash operation on data concatenated to a presentation** as equivalent to digital certificates, wherein. the certificate issuer name 301 is hashed at step 303, and at step 304, the hashed issuer name is concatenated with the certificate serial number 302 to produce the processed digital certificate 305. (The serial number could also be hashed before concatenation.) as taught by Kocher'509- see Kocher'509 col. 5 line 65 through col. 6 line 15.

Second: Appellant argues, **Smithies'835 and Kocher'509 do not teaches concatenating data to a representation and performing a second hash operation on the data concatenated to the representation as required by claim 1** (see the brief page 14 para 3 - the same arguments are substantially repeated for claims 2-20 pending –see the brief pages 17-22).

The examiner respectfully disagrees.

As discuss in the rejection above, using the broadest reasonable interpretation, it is noted **Smithies'835** teaches the Secure Hash Algorithm SHA-1, but does not expressly distinguish first and second hash; since SHA-1 is used for both "sign" and "affirm"; SHA-1 is hashed when "sign", and "affirm" an electronic document. It would have been obvious to one of ordinary skill in the art at the time of the invention to equates the **first hash and second hash** as equivalent to SHA-1 is used for both "sign" and "affirm". However, for further support, Kocher'509 discloses methods and apparatuses for constructing efficient cryptographically secure assertions as to whether candidate items are present on a list, includes the construction of a hash tree, wherein a verifier can determine the validity of the digital signature on the root node, and provides cryptographic assurance that the candidate data item is not on the list (see Kocher'509 col. 5 line 65 through col. 6 line 15). In addition, Kocher'509 in fig. 3 and col. 6 lines 40-50 discloses a particular preprocessing technique appropriate for data items such as digital certificates. The certificate issuer name 301 is hashed at step 303, and at step 304, the hashed issuer name is concatenated with the certificate serial number 302 to produce the processed digital certificate 305. (The serial number could also be hashed before concatenation.) For example, a certificate with a 32-bit (4-byte) serial number 123456789 whose CA name is "Sample CA" would have a

24-byte list entry consisting of SHA ("Sample CA") followed by the byte representation of 123456789. In particular, the hexadecimal representation would be: E2 CA 64 56 40 BE 99 AC CA 9D 3A 9B 02 97 0D 1E F2 95 8E A0 07 5B CD 15.)



Using the broadest reasonable interpretation, the examiner equates the claimed **a second hash operation on data concatenated to a presentation** as equivalent to digital certificates, wherein. the certificate issuer name 301 is hashed at step 303, and at step 304, the hashed issuer name is concatenated with the certificate serial number 302 to produce the processed digital certificate 305. (The serial number could also be hashed before concatenation.) as taught by Kocher'509- see Kocher'509 col. 5 line 65 through col. 6 line 15.

Third: Appellant argues, **Smithies'835 and Kocher'509 do not teach obtaining, recording, time stamping by a digital notary service of the representation of the contents of the electronic transcript and the data; and digitally signing the notary record; and forming an electronically signed electronic transcript by bundling the digitally signed notary record with the electronic transcript and with the data identifying the user as required by claim 1** (see the brief pages 15-17 - the same arguments are substantially repeated for claims 2-20 pending –see the brief pages 17-22).

The examiner respectfully disagrees.

As discuss in the rejection above, specifically, **Smithies'835** disclose the electronic transaction processing, and, in particular, to the field of computer-based recording or "transcribing" systems for collecting and storing data that evidences the facts and circumstances of a party's electronic affirmation of a document, transaction or event (e.g., the signing of an electronic document, the negotiation of an electronic sale, the affirmation of statements such as those recorded in a deposition, and the validation or verification of accountings, spreadsheets, applications, blueprints, government filings and other items) (see Smithies'835 col. 1 lines 15-30). In addition, the transcript object contains data from the following groups: Evidence to Provide a Link to Affirming Party, Evidence to Prove the Affirming Party's Intent, Evidence to Corroborate the Act of Signing or Affirmation, Evidence to Verify Integrity of the Provisions or Undertakings of a Document, Transaction or Statement, Evidence to Link the Specific Client Application to the Affirmation, and Evidence to Verify the Transcript Generator Module (see Smithies'835 col. 12 line 50 through col. 15 line 11). In addition, the term "affirm" as used

herein includes the act of signing a document, electronic or otherwise by any biometric, infometric or cryptographic means. The party may enter a handle, pointer or other access to a private key, which can be used to encrypt representations of the document and resulting transcript; this key will serve to verify the identity of the party. Also the term "affirmation" may also extend to events, (such as the transmission of a file or document), the occurrence of which may be recorded and stored in lieu of a traditional signature (see Smithies'835 col. 7 line 60 through col. 9, line 15). Using the broadest reasonable interpretation, the examiner equates the claimed **a digital notary service** as equivalent to electronic affirmation of a document, such as those recorded in a deposition, and the validation or verification of accountings, spreadsheets, applications, blueprints, government filings and other items) as taught by Smithies'835.

In addition, Kocher'509 in fig. 3 and col. 6 lines 40-50 discloses a particular preprocessing technique appropriate for data items such as digital certificates. The certificate issuer name 301 is hashed at step 303, and at step 304, the hashed issuer name is concatenated with the certificate serial number 302 to produce the processed digital certificate 305. (The serial number could also be hashed before concatenation.)

Using the broadest reasonable interpretation, the examiner equates the claimed **bundling the digitally signed notary record with the electronic transcript and with the data identifying the user** as equivalent to digital certificates, wherein the hashed issuer name is concatenated with the certificate serial number 302 to produce the processed digital certificate 305 as taught by Kocher'509, in view of electronic affirmation of a document, such as those recorded in a deposition, and the validation or verification of accountings, spreadsheets, applications, blueprints, government filings and other items) as taught by Smithies'835.

Fourth: Appellant argues, **Smithies'835 and Kocher'509 fail to establish prima facie case of obviousness** (see the brief page 17 para 2 - the same arguments are substantially repeated for claims 2-20 pending –see the brief pages 17-22).

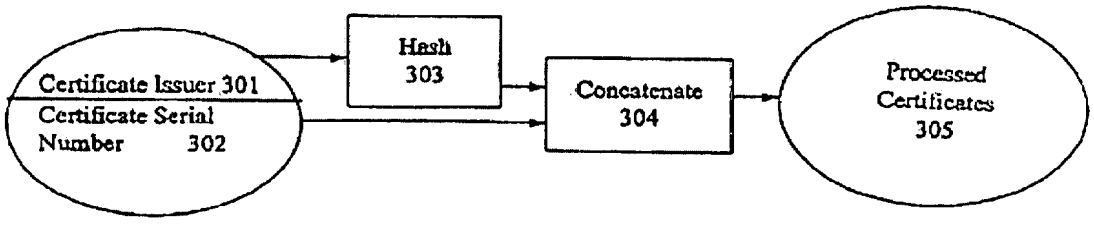
The examiner respectfully disagrees.

Following KSR direction as following: "SUPREME COURT OF THE UNITED STATES No. 04–1350 KSR INTERNATIONAL CO., PETITIONER v. TELEFLEX INC. ET AL. ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT [April 30, 2007], (page 2-3 of the court opinion) Following Graham v. John Deere Co. of Kansas City, 383 U. S. 1 (1966), the Court set out a framework for applying the statutory language of §103, language itself based on the logic of the earlier decision in Hotchkiss v. Greenwood, 11 How. 248 (1851), and its progeny. See 383 U. S., at 15–17. The analysis is objective:

> "Under §103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or nonobviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented." Id., at 17–18.

While the sequence of these questions might be reordered in any particular case, the factors continue to define the inquiry that controls. If a court, or patent examiner, conducts this analysis and concludes the claimed subject matter was obvious, the claim is invalid under §103. Seeking to resolve the question of obviousness with more uniformity and consistency, the Court of Appeals for the Federal Circuit has employed an approach referred to by the parties as the "teaching, suggestion, or motivation" test (TSM test), under which a patent claim is only proved obvious if "some motivation or suggestion to combine the prior art teachings" can be found in the prior art, the nature of the problem, or the knowledge of a person having ordinary skill in the art. See, e.g., Al-Site Corp. v. VSI Int'l, Inc., 174 F. 3d 1308, 1323–1324 (CA Fed. 1999). KSR challenges that test, or at least its application in this case. See 119 Fed. Appx. 282, 286–290 (CA Fed. 2005). Because the Court of Appeals addressed the question of obviousness in a manner contrary to §103 and our precedents, we granted certiorari, 547 U. S ___ (2006). We now reverse.

Using the broadest reasonable interpretation, and cites evidences above, the Examiner had found that Smithies'835 taught most of independent claim 1 limitations, but **Smithies'835** does not explicitly teach a second hash operation on data concatenated to a presentation. However, **Kocher'509** discloses methods and apparatuses for constructing efficient cryptographically secure assertions as to whether candidate items are present on a list, includes the construction of a hash tree, wherein a verifier can determine the validity of the digital signature on the root node, and provides cryptographic assurance that the candidate data item is not on the list (see Kocher'509 col. 5 line 65 through col. 6 line 15). In addition, Kocher'509 in fig. 3 and col. 6 lines 40-50, discloses a particular preprocessing technique appropriate for data items such as digital certificates. The certificate issuer name 301 is hashed at step 303, and at step 304, the hashed issuer name is concatenated with the certificate serial number 302 to produce the processed digital certificate 305. (The serial number could also be hashed before concatenation.) For example, a certificate with a 32-bit (4-byte) serial number 123456789 whose CA name is "Sample CA" would have a 24-byte list entry consisting of SHA ("Sample CA") followed by the byte representation of 123456789. In particular, the hexadecimal representation would be: E2 CA 64 56 40 BE 99 AC CA 9D 3A 9B 02 97 0D 1E F2 95 8E A0 07 5B CD 15.)



Using the broadest reasonable interpretation, the examiner equates the claimed **a second hash operation on data concatenated to a presentation** as equivalent to digital certificates, wherein. the certificate issuer name 301 is hashed at step 303, and at step 304, the hashed issuer name is concatenated with the certificate serial number 302 to produce the processed digital certificate 305. (The serial number could also be hashed before concatenation.) as taught by Kocher'509- see Kocher'509 col. 5 line 65 through col. 6 line 15.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Smithies'835 method of SHA-1 is hashed when "sign", and "affirm" an electronic document (see Smithies'835 col. 6 lines 55-65), to include a means of concatenating data to a representation and performing a second hash operation on the data concatenated to the representation as taught by Kocher'509. One of the ordinary skills in the art would have been motivated to modify this combination, because they are from the same field of endeavor of utilizing SHA-1 for hashing and validating the digital notary service of the representation of the contents of the electronic transcript and the data; and digitally signing the notary record; and forming an electronically signed electronic transcript by bundling the digitally signed notary record with the electronic transcript and with the data identifying the user and provides the benefit of demonstrating and confirming the status of a digital certificates and other data on a computer-implemented method (Kocher, Abstract section) and calling the transcript generator module to affirm a previously saved transcript object (Smithies, col 12, lines 40-42).

Thus the examiner has established a prima facie obviousness rejection of claim 1.

Therefore the Examiner respectfully maintains the rejection of claims 1-20 and should be sustained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Quoc A. Tran

6-19-2007

Conferees:

Stephen S. Hong (SPE)

William L. Bashore

Doug Hutton (SPE)